

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

CASE NO. 22-mj-8489-BER

IN RE SEALED SEARCH WARRANT

CRIMINAL COVER SHEET

1. Did this matter originate from a matter pending in the Northern Region of the United States Attorney's Office prior to August 8, 2014 (Mag. Judge Shaniek Maynard)? No
2. Did this matter originate from a matter pending in the Central Region of the United States Attorney's Office prior to October 3, 2019 (Mag. Judge Jared Strauss)? No

Respectfully submitted,

JUAN ANTONIO GONZALEZ
UNITED STATES ATTORNEY

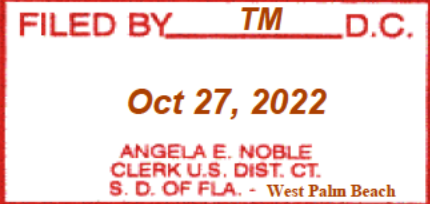
BY:

Assistant United States Attorney

99 Northeast 4th Street
Miami, Florida 33132-2111
Telephone: _____
E-mail: _____

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 22-mj-8489-BER



IN RE: SEARCH WARRANT

HIGHLY SENSITIVE DOCUMENT

MOTION TO SEAL

The United States of America, by and through the undersigned Assistant United States Attorney, hereby moves to seal this Motion, the Search Warrant, and all its accompanying documents, until further order of this Court. The United States submits that there is good cause because the integrity of the ongoing investigation might be compromised, and evidence might be destroyed.

The United States further requests that, pursuant to this Court's procedures for Highly Sensitive documents, all documents associated with this investigation not be filed on the Court's electronic docket because filing these materials on the electronic docket poses a risk to safety given the sensitive nature of the material contained therein.

Respectfully submitted,

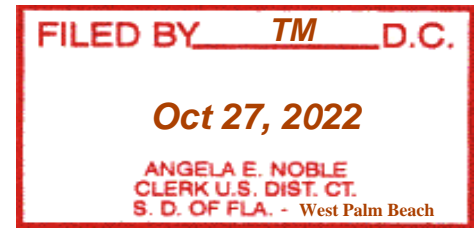
JUAN ANTONIO GONZALEZ
UNITED STATES ATTORNEY

BY:

[REDACTED]
Assistant United States Attorney
[REDACTED]
99 Northeast 4th Street
Miami, Florida 33132-2111
[REDACTED]

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 22-mj-8489-BER



IN RE: SEARCH WARRANT

HIGHLY SENSITIVE DOCUMENT

SEALING ORDER

The United States of America, having applied to this Court for an Order sealing the Motion to Seal, the Search Warrant and all its accompanying documents, and this order and the Court finding good cause:

IT IS HEREBY ORDERED that the Motion to Seal, the Search Warrant and its accompanying documents, and this Order shall be filed under seal until further order of this Court. However, the United States Attorney's Office and the Federal Bureau of Investigation may obtain copies of any sealed document for purposes of executing the search warrant.

DONE AND ORDERED in chambers at West Palm Beach, Florida, this 27 day of October 2022



HON. BRUCE E. REINHART
UNITED STATES MAGISTRATE JUDGE

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

IN RE: SEALED SEARCH WARRANT

Case No. 22-mj-8489-BER

Filed Under Seal

**APPLICATION FOR ORDER COMMANDING APPLE, INC.
NOT TO NOTIFY ANY PERSON OF THE EXISTENCE OF SEARCH WARRANT**

The United States respectfully requests that the Court order Apple, Inc. not to notify any person (including the subscribers or customers of the account listed in the search warrant) of the existence of the attached search warrant until further order of the Court.

Apple is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computer service, as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, the United States obtained the attached search warrant, which requires Apple to disclose certain records and information to the United States. This Court has authority under 18 U.S.C. § 2705(b) to issue “an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.” *Id.*

In this case, such an order would be appropriate because the attached search warrant relates to aspects of an ongoing criminal investigation that are neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the attached search warrant will seriously jeopardize the investigation, by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b)(2), (3), (5). Some of the evidence in this

investigation is stored electronically. If alerted to the investigation, the subjects under investigation could destroy that evidence, including information saved to their personal or business computers.

WHEREFORE, the United States respectfully requests that the Court grant the attached Order directing Apple not to disclose the existence or content of the attached search warrant, except that Apple may disclose the attached search warrant to an attorney for Apple, for the purpose of receiving legal advice.

The United States further requests that the Court order that this application and any resulting order be sealed for a period of one year. As explained above, these documents discuss aspects of an ongoing criminal investigation that are neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Executed on October 27, 2022.

Respectfully submitted,

JUAN ANTONIO GONZALEZ
ACTING UNITED STATES ATTORNEY

By:

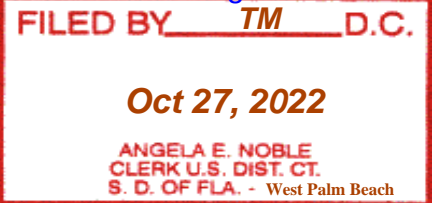
[REDACTED]

Assistant United States Attorney

[REDACTED]

99 Northeast 4th Street
Miami, Florida 33132-2111

[REDACTED]



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

IN RE: SEALED SEARCH WARRANT

Case No. 22-mj-8489-BER

Filed Under Seal

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2705(b), requesting that the Court issue an Order commanding Apple, Inc., an electronic communications service provider and/or a remote computing service, not to notify any person (including the subscribers or customers of the account listed in the search warrant) of the existence of the attached search warrant until further order of the Court.

The Court determines that there is reason to believe that notification of the existence of the attached search warrant will seriously jeopardize the investigation, by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b)(2), (3), (5).

IT IS THEREFORE ORDERED under 18 U.S.C. § 2705(b) that Apple shall not disclose the existence of the attached search warrant, or this Order of the Court, to the listed subscriber or to any other person, for a period of one year, except that Apple may disclose the attached search warrant to an attorney for Apple, for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court.

10/27/22
Date


HON. BRUCE E. REINHART
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT

for the
Southern District of FloridaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 22-mj-8489-BER

Information associated with Apple Destination Signaling
Identifier (DSID) [REDACTED] as further described in
Attachment A

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

FILED BY TM D.C.

Oct 27, 2022

ANGELA E. NOBLE
CLERK U.S. DIST. CT.
S. D. OF FLA. - West Palm Beach

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 793(e)
18 U.S.C. § 2071
18 U.S.C. § 1519
18 U.S.C. § 1001
18 U.S.C. § 1623

Offense Description

Willful retention of national defense information
Concealment or removal of government records
Obstruction of federal investigation
Material false statements
Perjury

The application is based on these facts:

See attached Affidavit of FBI Special Agent [REDACTED]

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

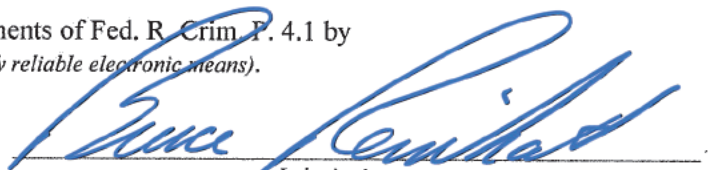
[REDACTED]

[REDACTED], Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Phone (WhatsApp) _____ (specify reliable electronic means).

Date: 10/27/2022


 Judge's signature

City and state: West Palm Beach, Florida

Hon. Bruce E. Reinhart, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, [REDACTED], being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with Apple Destination Signaling Identifier (DSID) [REDACTED] (the “TARGET ACCOUNT”) that is owned, maintained, controlled, or operated by Apple, Inc. (hereinafter “Apple”), a company headquartered at 1 Infinite Loop, Cupertino, California. The TARGET ACCOUNT is used by [REDACTED] and is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) [REDACTED]
[REDACTED] During this time, I have received training at the FBI Academy located at Quantico, Virginia, specific to counterintelligence and espionage investigations. [REDACTED]
[REDACTED] Based on my experience and training, I am familiar with efforts used to unlawfully collect, retain, and disseminate sensitive government information, including classified National Defense Information (“NDI”), and with efforts to obstruct justice.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the TARGET ACCOUNT, as described in Attachment A, contains evidence of violations of 18 U.S.C. § 793(e) (willful retention of national defense information); 18 U.S.C. § 2071 (concealment or removal of government records); 18 U.S.C. § 1519 (obstruction of federal investigation), 18 U.S.C. § 1001 (material false statement); or 18 U.S.C. § 1623 (perjury), as further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Background on Investigation

6. The FBI is investigating potential violations of 18 U.S.C. §§ 793(e), 2071, 1519, 1001, and 1623 related to the improper removal and storage of classified national defense information in unauthorized spaces, as well as the unlawful concealment or removal of government records.

7. This investigation began as a result of a referral that the United States National Archives and Records Administration (“NARA”) sent to the United States Department of Justice

(“DOJ”) on or about February 9, 2022 (hereinafter, the “NARA Referral”). The NARA Referral stated that on January 18, 2022, in accordance with the Presidential Records Act (“PRA”), NARA received from the office of former President Donald J. Trump (hereinafter “FPOTUS”), via representatives, fifteen (15) boxes of records (hereinafter, the “FIFTEEN BOXES”). The FIFTEEN BOXES, which had been transported from a property owned by FPOTUS at 1100 S. Ocean Blvd., Palm Beach, Florida, a residence and club known as “Mar-a-Lago,” were reported in the NARA Referral to contain, among other things, highly classified documents intermingled with other records.

8. After an initial review of the NARA Referral, the FBI opened a criminal investigation to, among other things, identify any person(s) who may have removed or retained classified information without authorization and/or in an unauthorized space. The FBI’s investigation established that documents bearing classification markings, which appear to contain NDI, were among the materials contained in the FIFTEEN BOXES and were stored at Mar-a-Lago in an unauthorized location.

9. As further described below, on May 11, 2022, the Department of Justice (“DOJ”) served a grand jury subpoena on counsel for the Office of the Former President (the “Office”) seeking “any and all documents . . . bearing classification markings” in FPOTUS’s and/or the Office’s possession. On June 3, 2022, FPOTUS’s counsel provided DOJ with a package of 37 documents bearing classification markings at the Confidential, Secret, and Top Secret level. Counsel for FPOTUS provided DOJ with a written certification, signed by another person who was acting as the custodian of records on behalf of the Office for purposes of the subpoena, indicating that “a diligent search was conducted,” that the “search was conducted after receipt of the subpoena, in order to locate any and all documents that are responsive to the subpoena” seeking

all documents with classification markings in the custody or control of FPOTUS and/or the Office, and that “any and all responsive documents” were being provided. Counsel for FPOTUS indicated that all responsive documents had been located in one storage room located on the ground floor at Mar-a-Lago (hereinafter, “the storage room.”).

10. After developing additional evidence that the June 3 production did not contain all of the documents with classification markings located at Mar-a-Lago, on August 8, 2022, the FBI executed a search and seizure warrant issued by a Magistrate Judge of the U.S. District Court for the Southern District of Florida. During the search, the FBI recovered from the storage room as well as FPOTUS’s office at Mar-a-Lago over 100 documents bearing classification markings, which had not been produced on June 3. The documents appeared to contain NDI. The search also yielded apparent government and/or Presidential records subject to the Presidential Records Act, 44 U.S.C. § 2201.

Background on NAUTA

11. NAUTA began his career in the U.S. Navy [REDACTED]
[REDACTED] NAUTA transitioned to work as a valet, or personal aide, for FPOTUS during FPOTUS’s Presidential Administration (hereinafter “Administration”). [REDACTED]
[REDACTED] In or around the summer of 2021, NAUTA retired from the military and went to work as a civilian for FPOTUS as his “body man” or assistant. According to publicly available information filed with the Federal Election Commission, the Save America PAC, a political action committee created by FPOTUS, paid NAUTA \$149,167 between August 26, 2021 and August 30, 2022, which included \$6,375 in “advance consulting” fees.

12. NAUTA was involved in at least two key movements of FPOTUS's boxes at Mar-a-Lago: (1) in the weeks leading up to the provision of the FIFTEEN BOXES to NARA in January 2022, NAUTA and two other FPOTUS employees brought, at FPOTUS's request, the FIFTEEN BOXES from their location in a storage room at Mar-a-Lago to FPOTUS's residential entryway at Mar-a-Lago for FPOTUS's review; and (2) in the week before FPOTUS's representatives claimed on June 3 that they had conducted a diligent search for classified documents, NAUTA moved approximately 64 boxes out of the storage room at Mar-a-Lago and returned only about 25-30 prior to the review of the storage room for records responsive to the May 11 subpoena. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

13. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

14. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

15.

[REDACTED]

16.

[REDACTED]

17.

[REDACTED]

[REDACTED]

[REDACTED] The door to the storage room was painted gold and had no other markings on it.

18. In addition to the approximately eighty-five to ninety-five FPOTUS BOXES located in the storage room, there were also other boxes in the storage room with merchandise such as challenge coins, garment bags, memorabilia from Mar-a-Lago such as photograph frames, and other décor items.

Provision of the Fifteen Boxes to NARA

19. Over the course of 2021, NARA endeavored to obtain what appeared to be missing records subject to the Presidential Records Act (PRA), 44 U.S.C. § 2201. On or about May 6, 2021, NARA made a request for the missing PRA records and continued to make requests until approximately late December 2021, when NARA was informed twelve boxes were found and ready for retrieval at Mar-a-Lago. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

20. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

21. [REDACTED] took a photograph of the storage room and provided it to FPOTUS sometime between January 1-17, 2022, to show FPOTUS the number of boxes that were in the

storage room. The storage photo, which appears below [REDACTED]

[REDACTED] captures approximately sixty-one of the FPOTUS BOXES located in the storage room:



22. [REDACTED]

[REDACTED]

23. [REDACTED]

[REDACTED]

24.

[REDACTED]

25.

[REDACTED]

26.

[REDACTED]

27.

[REDACTED]

28. From May 16-18, 2022, FBI agents conducted a preliminary review of the FIFTEEN BOXES provided to NARA and identified over 100 documents with classification

markings in fourteen of the FIFTEEN BOXES. Several of the documents also contained what appears to be FPOTUS's handwritten notes.

Grand Jury Subpoena, Related Correspondence, and Production of Additional Classified Documents

29. On May 11, 2022, an attorney representing FPOTUS, "FPOTUS COUNSEL 1," agreed to accept service of a grand jury subpoena requesting "[a]ny and all documents or writings in the custody or control of Donald J. Trump and/or the Office of Donald J. Trump bearing classification markings." The return date of the subpoena was May 24, 2022.

30. After an extension was granted for compliance with the subpoena, on the evening of June 2, 2022, FPOTUS COUNSEL 1 contacted DOJ COUNSEL and requested that FBI agents meet him the following day to pick up responsive documents. On June 3, 2022, three FBI agents and DOJ COUNSEL arrived at Mar-a-Lago to accept receipt of the materials. In addition to FPOTUS COUNSEL 1, another individual, hereinafter "INDIVIDUAL 2," was also present as the custodian of records for FPOTUS's post-presidential office. The production included a single Redweld envelope, wrapped in tape, containing documents. FPOTUS COUNSEL 1 relayed that the documents in the Redweld envelope were found during a review of the boxes located in the storage room. INDIVIDUAL 2 provided a Certification Letter, signed by INDIVIDUAL 2, which stated the following:

Based upon the information that has been provided to me, I am authorized to certify, on behalf of the Office of Donald J. Trump, the following: a. A diligent search was conducted of the boxes that were moved from the White House to Florida; b. This search was conducted after receipt of the subpoena, in order to locate any and all documents that are responsive to the subpoena; c. Any and all responsive documents accompany this certification; and d. No copy, written notation, or reproduction of any kind was retained as to any responsive document.

31. During receipt of the production, FPOTUS COUNSEL 1 stated he was advised all the records that came from the White House were stored in the storage room at Mar-a-Lago and the boxes of records in the storage room were “the remaining repository” of records from the White House. FPOTUS COUNSEL 1 further stated he was not advised there were any records in any private office space or other location in Mar-a-Lago. The agents and DOJ COUNSEL were permitted to see the storage room (although they were not permitted to look inside the boxes) and observed that approximately fifty to fifty-five boxes remained in the storage room. Considering that only FIFTEEN BOXES had been provided to NARA of the approximately eighty-five to ninety-five FPOTUS BOXES that had been located in the storage room, it appeared that approximately fifteen to thirty of the FPOTUS BOXES had previously been relocated elsewhere. The FBI agents also observed that the composition of boxes differed such that fewer Bankers boxes were visible, while more plain cardboard boxes and storage bins were present. Other items were also present in the storage room, including a coat rack with suit jackets, as well as interior décor items such as wall art and frames.

32. [REDACTED]

[REDACTED]

[REDACTED]

33. A review of the documents contained in the Redweld envelope produced pursuant to the grand jury subpoena revealed 37 unique documents bearing classification markings, some of which bore classification markings at the highest levels. Based on my training and experience, I know that documents classified at these levels typically contain NDI. Multiple documents also contained what appears to be FPOTUS’s handwritten notes.

34. When producing the documents, neither FPOTUS COUNSEL 1 nor INDIVIDUAL 2 asserted that FPOTUS had declassified the documents.¹ The documents being in a Redweld envelope wrapped in tape appears to be consistent with an effort to handle the documents as if they were still classified.²

Surveillance Camera Footage Shows NAUTA removing boxes from the Storage Room Area Prior to FPOTUS Counsel 1's Review in Connection with the Subpoena

35. On July 6, 2022, in response to a grand jury subpoena for surveillance video from internal cameras located on the ground floor (basement) [REDACTED] representatives of the Trump Organization provided a hard drive to FBI agents. Upon review of the hard drive, the FBI determined that the drive contained video footage from four cameras in the basement hallway of Mar-a-Lago in which the door to the storage room is located. The footage on the drive begins on April 23, 2022, and ends on June 24, 2022. The recording feature of the cameras appears to be motion activated, so that footage is only captured when motion is detected within each camera's field of view.

¹ 18 U.S.C. § 793(e) does not use the term "classified information," but rather criminalizes the unlawful retention of "information relating to the national defense." The statute does not define "information related to the national defense," but courts have construed it broadly. *See Gorin v. United States*, 312 U.S. 19, 28 (1941) (holding that the phrase "information relating to the national defense" as used in the Espionage Act is a "generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness"). In addition, the information must be "closely held" by the U.S. government. *See United States v. Squillacote*, 221 F.3d 542, 579 (4th Cir. 2000) ("[I]nformation made public by the government as well as information never protected by the government is not national defense information."); *United States v. Morison*, 844 F.2d 1057, 1071-72 (4th Cir. 1988). Certain courts have also held that the disclosure of the documents must be potentially damaging to the United States. *See Morison*, 844 F.2d at 1071-72.

² On May 25, 2022, while negotiating for an extension of the subpoena, FPOTUS COUNSEL 1 sent two letters to DOJ COUNSEL. In the second such letter, available at 22-mj-8332-BER (D.E. 125), FPOTUS COUNSEL 1 asked DOJ to consider a few "principles," which include FPOTUS COUNSEL 1's claim that a President has absolute authority to declassify documents. In this letter, FPOTUS COUNSEL 1 requested, among other things, that "DOJ provide this letter to any judicial officer who is asked to rule on any motion pertaining to this investigation, or on any application made in connection with any investigative request concerning this investigation."

36. One camera in particular, identified on the hard drive as “South Tunnel Liquor,” provides a view of entry and exit into a room (hereafter anteroom) that leads to the storage room. The doorway to the anteroom itself is not visible in the camera view, as a refrigerator is directly between the camera and doorway, but the footage from this camera nonetheless establishes entry and exit to the anteroom because it is apparent when persons within the camera’s field of view turn directly behind the refrigerator and then disappear from view. The anteroom, in addition to its entrance from the South Tunnel, has approximately four doors leading off it, one of which is the gold-painted door that leads to the storage room. The anteroom provides the only entrance to the storage room; however, other offices can also be entered from the anteroom, so it might be possible for persons to enter the storage room from those other offices without being visible in the surveillance camera footage.

37. By reviewing the camera footage provided by the Trump Organization in response to the subpoena, the FBI has determined the following:

On May 24, 2022, NAUTA is observed exiting the anteroom doorway with three boxes.

On May 30, 2022, four days after NAUTA’s interview with the FBI during which the location of boxes was a significant subject of questioning, NAUTA is observed exiting the anteroom doorway with approximately fifty Bankers boxes, consistent with the description of the FPOTUS BOXES. FBI did not observe this quantity of boxes being returned to the storage room through the anteroom entrance in its review of the footage.

On June 1, 2022, NAUTA is observed carrying eleven brown cardboard boxes out the anteroom entrance. One box did not have a lid on it and appeared to contain papers.

The day after that, on June 2, 2022, NAUTA is observed moving twenty-five to thirty boxes, some of which were brown cardboard boxes and others of which were Bankers boxes consistent with the description of the FPOTUS BOXES, into the entrance of the ANTEROOM. Approximately three and a half hours later, NAUTA is observed escorting FPOTUS COUNSEL 1 in through the entrance of the anteroom, and FPOTUS COUNSEL 1 is not observed leaving until approximately two and a half hours later.

On June 3, 2022, FPOTUS COUNSEL 1 is escorted through the anteroom entrance by an unidentified individual wearing a jacket with "USSS POLICE" printed on the back. The unidentified individual and FPOTUS COUNSEL 1 exit the ANTEROOM entrance moments later. FPOTUS COUNSEL 1 appeared to be carrying a Redweld envelope after exiting the anteroom.

38. According to FBI's review of video footage, and as detailed in the paragraph above, NAUTA can be observed removing approximately 64 boxes from the storage room area between May 24 and June 1, 2022, but only returning 25-30 boxes to the storage room area on June 2, 2022. Notably, and as described above in paragraph 28, these boxes were removed following service of a grand jury subpoena but before FPOTUS COUNSEL 1's review of boxes in the storage room area to locate documents responsive to the subpoena.

39. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

NAUTA concealed information during his FBI interview [REDACTED]

40. On May 26, 2022, the FBI interviewed NAUTA and explained that the FBI was conducting an investigation as to whether classified documents were stored at Mar-a-Lago and that the FBI was particularly interested in where the boxes with classified documents were located and whether they had been moved outside the storage room.

41. [REDACTED] During the interview, NAUTA claimed that the first time NAUTA saw the boxes was when NAUTA moved them from Pine Hall, the anteroom to FPOTUS's personal residential suite, to the moving truck to provide the boxes to NARA. [REDACTED]

[REDACTED]

[REDACTED] Further, in NAUTA's interview with the FBI on May 26, he had stated that he did not know where the boxes had come from prior to being located in Pine Hall. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

42. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

43. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Execution of Search Warrant at Mar-a-Lago and Movement of Boxes After June 3

44. On August 8, 2022, the FBI executed a search warrant at Mar-a-Lago authorized by the Honorable Bruce E. Reinhart, U.S. Magistrate Judge in the Southern District of Florida. *See* 22-mj-83332-BER. The search yielded over 100 unique documents bearing classification markings, with some indicating the highest levels of classification and extremely limited distribution, found in both the storage room and FPOTUS's office at Mar-a-Lago. Based on my training and experience, I know that documents classified at these levels typically contain NDI.

45. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

46. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

47. [REDACTED]

[REDACTED]

The TARGET ACCOUNT

48. On September 30, 2022, [REDACTED] Apple provided records which confirmed [REDACTED] has been the registered user of the TARGET ACCOUNT [REDACTED]. Apple records also list [REDACTED] as the telephone number associated with the TARGET ACCOUNT, [REDACTED] as the email address associated with the TARGET ACCOUNT, iCloud as a service for the TARGET ACCOUNT, and an iPhone 13 Pro Max as the device associated with the TARGET ACCOUNT [REDACTED].

49. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

50. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

51. On September 30, 2022, open-source research revealed that [REDACTED] phone number [REDACTED] was registered with WhatsApp, an encrypted communication application. In my training and experience, WhatsApp permits users to back up communications to a cloud service and accordingly, there may be stored communications through backed-up WhatsApp messages on the TARGET ACCOUNT.

52. Based upon this investigation, I believe that there may be stored communications within the TARGET ACCOUNT that contain evidence detailing the removal of FPOTUS boxes, which likely contained classified information and NDI, from the White House to Mar-a-Lago and from the storage room at Mar-a-Lago. Furthermore, I believe there may be stored communications in the TARGET ACCOUNT detailing efforts to mislead law enforcement. Finally, the data from the TARGET ACCOUNT would also provide location information [REDACTED] that could indicate when and where [REDACTED] moved boxes, such as if [REDACTED] moved the boxes to a storage facility or other location outside of Mar-a-Lago. As indicated below, Apple has location services that could be used to determine where a user traveled with the user's phone.

INFORMATION REGARDING APPLE³

53. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

54. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

55. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

56. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

57. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

³ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

58. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

59. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

60. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

61. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

62. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital

content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

63. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

64. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

65. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and

utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

66. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

67. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

68. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

69. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

70. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in

furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

71. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

72. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

73. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity,

documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

74. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

REVIEW OF THE INFORMATION OBTAINED PURSUANT TO THE WARRANT

75. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to Apple, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 14 days from the date of service. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts in the governments control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section II of Attachment B to the proposed warrant.

76. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the TARGET ACCOUNT. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly using keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that a law enforcement officer is likely to search for.

CONCLUSION

77. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR NON-DISCLOSURE AND SEALING

78. The United States request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss aspects of an ongoing criminal investigation that are neither public nor known to the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.


79. The United States further requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), Apple be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for a period of one year. The United States submits that such an order is justified because notification of the existence of this Order would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscribers an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution.

FILTER PROCEDURES

80. [REDACTED] has been represented by attorneys in this matter since at least in or around [REDACTED]. A Filter Team will review seized communications and segregate potentially protected materials, i.e., communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. The Filter Team will have no future involvement in the investigation of this matter. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its

review. If at any time the government identifies seized materials that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents can review the potentially privileged documents. If the Filter Team concludes that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team. The government believes that the subject of the search is not aware of this warrant. If possible, government attorneys will engage with the privilege holder to resolve privilege determinations before proceeding to court for judicial review.

Respectfully submitted,


Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1
by telephone (WhatsApp) this 27 day of October, 2022


HON. BRUCE E. REINHART
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple Destination Signaling Identifier (DSID) [REDACTED] that is owned, maintained, controlled, or operated by Apple Inc., a company headquartered at 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, Inc (“the Provider”), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile

Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud

Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All search history or web history;

i. All records pertaining to the types of service used;

j. All usernames associated with or sharing a login IP address or browser cookie with the account;

k. All cookies, including third-party cookies, associated with the user;

l. All records that are associated with the machine cookies associated with the user;

m. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

n. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence, and/or instrumentalities of violations of 18 U.S.C. § 793 (willful retention of national defense information); 18 U.S.C. § 2071 (concealment or removal of government records); 18 U.S.C. § 1519 (obstruction of federal investigation); 18 U.S.C. § 1001 (material false statement); or 18 U.S.C. § 1623 (perjury) [REDACTED], since January 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Communications, records, documents, and other files regarding the access to or movement or location of any boxes or records;
- (b) Information, including communications in any form, regarding the retrieval, storage, or transmission of national defense information or classified material;
- (c) Information, including communications in any form, regarding any government and/or Presidential records created between January 20, 2017, and January 20, 2021;
- (d) Any evidence of the knowing alteration, destruction, or concealment of any government and/or Presidential records, or of any documents with classification markings;
- (e) Communications, records, documents, and other files regarding the source and nature of any monetary transactions;
- (f) Evidence indicating how and when the account was accessed or used to determine the context of account access, use, and events relating to the crimes under investigation and to the account owner;

- (g) Evidence establishing the motive, capability, or willingness to commit the above-referenced crimes, including but not limited to evidence indicating the account owner's state of mind as it relates to the crimes under investigation;
- (h) The identity of the person(s) who communicated with the account user about matters relating to violations of the above-referenced crimes, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the
Southern District of Florida

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)) Case No. 22-mj-8489-BER
Information associated with Apple Destination Signaling)
Identifier (DSID) [REDACTED], as further described in)
Attachment A)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before November 10, 2022 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____
Duty Magistrate
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued:

10/27/22 16:33


Judge's signature

City and state:

West Palm Beach, FL

Hon. Bruce E. Reinhart, U.S. Magistrate Judge

Printed name and title

ReturnCase No.:
22-mj-8489-BER

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Apple Destination Signaling Identifier (DSID) [REDACTED] that is owned, maintained, controlled, or operated by Apple Inc., a company headquartered at 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, Inc (“the Provider”), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile

Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud

Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All search history or web history;

i. All records pertaining to the types of service used;

j. All usernames associated with or sharing a login IP address or browser cookie with the account;

k. All cookies, including third-party cookies, associated with the user;

l. All records that are associated with the machine cookies associated with the user;

m. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

n. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence, and/or instrumentalities of violations of 18 U.S.C. § 793 (willful retention of national defense information); 18 U.S.C. § 2071 (concealment or removal of government records); 18 U.S.C. § 1519 (obstruction of federal investigation); 18 U.S.C. § 1001 (material false statement); or 18 U.S.C. § 1623 (perjury) [REDACTED], since January 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Communications, records, documents, and other files regarding the access to or movement or location of any boxes or records;
- (b) Information, including communications in any form, regarding the retrieval, storage, or transmission of national defense information or classified material;
- (c) Information, including communications in any form, regarding any government and/or Presidential records created between January 20, 2017, and January 20, 2021;
- (d) Any evidence of the knowing alteration, destruction, or concealment of any government and/or Presidential records, or of any documents with classification markings;
- (e) Communications, records, documents, and other files regarding the source and nature of any monetary transactions;
- (f) Evidence indicating how and when the account was accessed or used to determine the context of account access, use, and events relating to the crimes under investigation and to the account owner;

- (g) Evidence establishing the motive, capability, or willingness to commit the above-referenced crimes, including but not limited to evidence indicating the account owner's state of mind as it relates to the crimes under investigation;
- (h) The identity of the person(s) who communicated with the account user about matters relating to violations of the above-referenced crimes, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple, and my title is _____ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. The process or system is regularly verified by Apple, and at all times pertinent to the records certified here, the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature